REMARKS

The present application was filed on September 15, 2005, with claims 1-40. The present application claims priority to PCT application US04/21846, filed July 9, 2004, and U.S. provisional application Serial No. 60/486,127, filed July 10, 2003. Claims 1-40 remain pending in the present application.

The specification has been objected to based on trademark usage.

Claim 15 is rejected under 35 U.S.C. §112, second paragraph, as being indefinite.

Claims 1, 5, 6, 13, 19 and 35-40 are rejected under 35 U.S.C. §103(a) over U.S. Patent No. 6,230,269 (hereinafter "Spies").

Claims 2-4, 7-12, 14-18 and 20-34 are each rejected under 35 U.S.C. §103(a) over Spies in view of one or more other cited references.

In this response, Applicants traverse the objection to the specification, traverse the §112 and §103(a) rejections, and amend the specification and claims 15 and 37-40.

With regard to the objection to the specification, it is believed that the trademark usage in the application as originally filed is appropriate. It is important to note that, at the time the application was filed, the trademarks in question were all registered trademarks, and are clearly identified as such directly in the application. It should also be noted that these trademarks are owned by the assignee of the present application. Moreover, corresponding generic terminology is present in the application for each trademark. For example, generic terminology corresponding to the ACE/Agent trademark is software for use in transmitting authentication information. See the specification at page 1, lines 27-29. The objection to the specification based on trademark usage is therefore believed to be improper and should be withdrawn.

Notwithstanding the traversal, Applicants have amended the specification in order to fully capitalize each of the trademarks in question.

With regard to the §112 rejection, the Examiner argues that the term "management command" in claim 15 is indefinite. Applicants respectfully disagree. The specification at page 6, lines 7-11, clearly provides as follows, with emphasis supplied:

> The SSGP protocol may be initiated, for example, by the SSGP server responsive to receipt of a management command from another entity of the system 100, by the SSGP server responsive to receipt of a request initiated by the SSGP client, or by any other suitable initiation mechanism.

Thus, it is clear that the recited management command may be a command generated by an entity of the system 100 other than the SSGP server 110S in order to control initiation of the SSGP protocol described in the specification. Claims are considered to be definite, as required by the second paragraph of 35 U.S.C. §112, when they define the metes and bounds of a claimed invention with a reasonable degree of precision and particularity. See In re Venezia, 530 F.2d 956, 958, 189 USPQ 149, 151 (CCPA 1976). In the present application, the scope of claim 15 which utilizes the term in question can be ascertained with a reasonable degree of precision and particularity, and therefore the objection should be withdrawn.

Notwithstanding the traversal, Applicants have made a broadening amendment to claim 15 by replacing the term "management command" with just the word --command--.

With regard to the §103(a) rejection over Spies, the Examiner argues that each and every limitation in claims 1, 5, 6, 13, 19 and 35-40 is taught or suggested by Spies. Applicants respectfully disagree.

Independent claim 1 is directed to a method for secure generation of a seed for use in performing one or more cryptographic operations. The method includes the steps of a seed generation server providing a first string to a seed generation client, the seed generation client generating a second string, encrypting the second string utilizing a key, and sending the encrypted second string to the seed generation server, the seed generation client generating the seed as a function of at least the first string and the second string, and the seed generation server decrypting the encrypted second string and independently generating the seed as a function of at least the first string and the second string.

The ability of the seed generation server to independently generate the seed as a function of the first and second strings is an important advantage of the claimed arrangement. For example, this type of arrangement advantageously overcomes the problems associated with conventional practice as described in the specification at page 2, lines 1-14, page 3, lines 10-13, and page 6, lines 5-7.

The Examiner in formulating the §103(a) rejection of claim 1 acknowledges that the Spies reference fails to teach or suggest the recited seed generation server that independently generates the seed as a function of at least the first string and the second string, as is expressly recited in claim 1. See the Office Action at page 4, second full paragraph. However, the

Examiner argues that it would be obvious to modify Spies to incorporate such a feature. Applicants respectfully disagree, for the reasons outlined below.

The Examiner apparently argues that the seed recited in claim 1 is met by the seed specified in Spies at column 7, lines 41-44. This seed generated by client 26 includes four distinct values, namely, H(1D), H(ID/P), P and S, where H(1D) denotes a hash of a user identifier, H(ID/P) denotes a hash of the user identifier concatenated with a user password, P denotes the user password, and S denotes key source material sent from the server 22 to the client 26. However, the server 22 in Spies does not and cannot independently generate this seed. This is because the Spies system is specifically designed such that the server does not know the user password P. See Spies at, for example, column 7, line 64, to column 8, line 8, which provides as follows with emphasis supplied:

> The system is secure because only the user knows his/her own password and this password is not required to be stored on any machine. Even the trusted authentication server does not know the user's password since it receives only a hash value of the password. Thus, the authentication server cannot secretly authenticate messages on behalf of the user. Additionally, the password P and key source material S are exchanged between the client and server in an encrypted form. An eavesdropper is prevented from intercepting the transmission and discovering the password P and source material S in their raw forms.

Accordingly, the Spies system is specifically designed such that its security depends on the server 22 not being able to generate the same seed, comprising the four values H(1D), H(ID/P), P and S, that is generated by the client 26. This is in direct contrast to the claimed arrangement, wherein the goal is to have both the server and client securely generate the same seed. Compare Spies at column 7, lines 63-64, and column 2, lines 5-20, with the present specification at page 2, lines 1-14, page 3, lines 10-13, and page 6, lines 5-7.

The Examiner states that one skilled in the art would be motivated to modify Spies to allow the server 22 to generate the same seed, comprising the four values H(ID), H(1D/P), P and S, that is generated by the client 26, because to do so would allegedly "increase the security of the seed generation protocol" in Spies by allowing the server 22 "to validate that the seed was generated by the client correctly." See the Office Action at page 4, last paragraph. However, as indicated above, the security of the Spies system clearly depends on the server 22 not being able to generate the same four-value seed as the client 26. Thus, if Spies were indeed modified in the

manner suggested by the Examiner, the resulting system would in fact be less secure and not more secure as alleged. See the above-quoted portion of Spies at column 7, line 64, to column 8, line 8. Moreover, such a modification would appear to render the Spies system unsuitable for one of its primary stated purposes, which is avoiding the need to store private information of multiple clients on a central server. See Spies at, for example, column 2, lines 11-20, and column 7, lines 63-64.

Applicants therefore respectfully submit that the proffered statement of motivation is a conclusory statement of the sort rejected by both the Federal Circuit and the U.S. Supreme Court. See KSR v. Teleflex, 127 S. Ct. 1727, 1741 (2007), quoting In re Kahn, 441 F. 3d 977, 988 (Fed. Cir. 2006) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness."). There has been no showing in the present §103(a) rejection of claim 1 of objective evidence of record that would motivate one skilled in the art to modify Spies to incorporate a feature whereby a server can independently generate the same seed as that generated by the client using first and second strings. To the contrary, as outlined above, Spies itself teaches directly away from the proposed modification by indicating that the security of its system would be seriously undermined if such a modification were made.

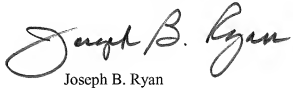
Independent claims 35 and 36 include seed generation server limitations similar to those of claim 1, and are believed allowable for reasons similar to those outlined above in the context of claim 1.

Dependent claims 2-34 are believed allowable at least by virtue of their dependence from claim 1, and are also believed to define separately-patentable subject matter. The additional references cited by the Examiner fail to supplement the fundamental deficiencies of the Spies reference as applied to claim 1.

Independent claims 37-40 have been amended to clarify the subject matter which Applicants regard as the invention. More specifically, each of these claims has been clarified to indicate that both the seed generation client and the seed generation server generate the same seed as a function of at least the first string and the second string. For the reasons noted above in the context of claim 1, such arrangements would not be obvious in view of the Spies reference, taken alone or in combination with the other cited art.

In view of the foregoing, claims 1-40 as amended are believed to be in condition for allowance.

Respectfully submitted,



Date: December 26, 2008

Joseph B. Ryan
Attorney for Applicant(s)
Reg. No. 37,922
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-7517